Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, DC 20554

In the Matter of	)	
	)	
PRIVACY AND SECURITY OF INFORMATION STORED ON MOBILE COMMUNICATIONS DEVICES	)	**CC Docket No. 96-115**
	)	
	)	
	)	
	)	

COMMENTS OF

GREEK ORTHODOX ARCHDIOCESE OF AMERICA

UNITED CHURCH OF CHRIST OFFICE OF OC, INC.

UNITED STATES CONFERENCE OF CATHOLIC BISHOPS

Introduction

The Greek Orthodox Archdiocese of America, United Church of Christ's Office of Communication, Inc. and the United States Conference of Catholic Bishops welcome this opportunity to comment on the privacy and security of information stored on mobile communications devices.

We represent over 65 million Americans in more than 18,000 thousand congregations and parishes throughout the U.S., which are home for hundreds of thousands of households of families with children. As people of faith, we believe that parents have primary responsibility for children's growth and formation. In this effort, it is then essential that parents be aware of and understand the information that is being collected in their use of mobile devices. Therefore, we encourage both the Commission and industry to give primary importance to ensuring consumers fully understand the privacy policies for mobile devices their families use.

Background

The question of the privacy of consumer data is currently the subject of many policy discussions. There is a growing sentiment that additional safeguards on consumer privacy are greatly needed. Several bills in Congress that seek to protect consumer privacy in the online and mobile world.[1] Earlier this year, the Administration released a Consumer Privacy Bill of Rights, which calls for protection of consumer rights such as individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.

[1] *See H.R.1895 Do Not Track Kids Act of 2011, available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.1895: and *S.913 Do-Not-Track Online Act of 2011, available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.00913:

In February of this year, the Federal Trade Commission reported that parents cannot determine which mobile apps pose privacy risks to their children before downloading the app.[2] One month later, the FTC issued a report with recommendations on consumer privacy protection, reporting that the FTC has "… sued dozens of companies that broke their privacy and security promises".[3] The FTC report proposed the following practices:

- Privacy by Design: Build in privacy at every stage of product development;
- Simplified Choice for Businesses and Consumers: Give consumers the ability to make decisions about their data at a relevant time and context …while reducing the burden on businesses of providing unnecessary choices; and
- Greater Transparency: Make information collection and use practices transparent.[4]

At a recent Senate Commerce Committee hearing, Ohio State University law professor Peter Swire, who served as the White House privacy adviser during the Clinton administration, said his research shows that industry self-regulation only works when Congress or the administration is focused on privacy. "Industry works a lot harder at this when government is paying attention." [5]

We believe the proposed legislation in Congress, as well as the actions of the Administration and the FTC all point to a need for greater consumer information and control about the data collected by online and mobile companies.

---

[2] *See Mobile Apps for Kids: Current Privacy Disclosures are Dis*appo*inting*, Federal Trade Commission (February 2012) *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

[3] *See Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Federal Trade Commission (March 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[4] Ibid.

[5] *See* Rockefeller Says He Doesn't Trust Industry to Regulate Itself on Privacy, by Juliana Gruenwald, *National Journal* (June 28, 2012), *available at* http://techdailydose.nationaljournal.com/2012/06/rockefeller-says-he-doesnt-tru.php

Response to Commission's Questions

The foundational principle that guides our response to all of the Commission's questions is that consumers must not only have access to the information that is being collected about them on mobile devices, but this information must be clearly provided and explained. In addition, consumers must always clearly understand how they might opt-out of information collection.

In its Notice, the Commission asks:

- *Are consumers given meaningful notice and choice with respect to service providers' collection of usage-related information on their devices?* We do not believe that consumers are given meaningful notice and choice. Our experience is that the families in our communities are rarely informed of the information being collected about them on their mobile devices. We also encourage the Commission to explore providing consumers with an option to opt-in for data collection, in which providers can only collect data with explicit consent of consumers, in addition to the current opt-out model.
- *What role can disclosure of service providers' practices to wireless consumers play?* Disclosure of service providers' practices to wireless consumers is crucial. This disclosure should not simply be provided in the service provider's literature, but also much more clearly stated at the point of sale. This is essential because the provider has an advantage in that many consumers are not savvy in the area of data collection. They are often not aware that it is happening and not able to understand technical literature in which it is explained. Therefore the provider has a responsibility to provide this information in terms that are accessible to the consumer.

- *Do current practices serve the needs of service providers and consumers, and in what ways?* We believe that current practices serve the needs of providers much more than the needs of consumers, since providers are able to obtain the data they seek but consumers are usually not aware the data is being collected. We advocate a more even balance in knowledge and information sharing on the part of providers to consumers, since providers' needs seem – at present - to have primary place.
- *To what extent should consumers bear responsibility for the privacy and security of data in their custody or control?* We believe that consumers have responsibility for safeguarding their data, but that their uneven understanding of the technical aspects of data sharing and collecting make it difficult for them to be aware of all that may be at stake. They can only truly assume their responsibility to the extent that they are informed in accessible language of the nature of the issue, their options for dealing with the choices they have, and how to take action effectively.

Ultimately, success in this arena requires a partnership between service providers, consumers and government. We do not seek to place the full burden on service providers. We recognize there is a legitimate need for data related to improve the quality of wireless services. But consumer awareness of the data collection is an essential element for a functional partnership.

Conclusion

We commend the Commission for its leadership in undertaking this process and stand ready to assist in any way we can to ensure the privacy of all Americans in their use of mobile devices.

Respectfully submitted,

Helen Osman
Secretary for Communications
U.S. Conference of Catholic Bishops
3211 4th St NE
Washington, DC 20017
202.541.3320

July 12, 2012